UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE

ANDREA RAWLINSON, on behalf of her minor children J.W. and A.B., and on behalf of all others similarly situated, Plaintiff, v. **CDHA MANAGEMENT, LLC, d/b/a CHORD SPECIALTY DENTAL PARTNERS and SPARK DSO, LLC d/b/a CHORD SPECIALTY DENTAL PARTNERS,** Defendant.	Case No. _____ CLASS ACTION **DEMAND FOR JURY TRIAL**

Andrea Rawlinson ("Plaintiff"), through her attorneys, on behalf of her minor children J.W and A.B. and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant CDHA Management, LLC d/b/a Chord Specialty Dental Partners and Spark DSO, LLC d/b/a Chord Specialty Dental Partners ("Chord" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiff alleges the following on information and belief—except as to her own actions, counsel's investigations, and facts of public record.

NATURE OF ACTION

1. This class action arises from Chord's failure to protect highly sensitive data.

2. Chord is a dental support company based in Tennessee that provides services to more than 60 dental practices throughout six states.[1]

[1] https://www.chordsdp.com/about/ (last visited April 03, 2025).

3. As such, Defendant stores a litany of highly sensitive personal identifiable information ("PII") and protected health information ("PHI") (collectively "PII/PHI") about its current and former patients. But Defendant lost control over that data when cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the "Data Breach").

4. Upon information and belief, the Data Breach impacted at least 173,430 individuals.[2] And, upon information and belief, the victims of the Data Breach included Defendant's current and former patients.

5. According to Defendant's Breach Notice, between August 19, 2024 and September 25, 2024, Defendant was the target of a cyberattack. In other words, Chord had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to its current and former patients' PII/PHI.

6. On information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class's PII/PHI. In short, Defendant's failures placed the Class's PII/PHI in a vulnerable position—rendering them easy targets for cybercriminals.

7. Plaintiff is a Data Breach victim, having received a breach notice—a copy of Defendant's Breach Notice is attached as Exhibit A. She brings this class action on behalf of her two minor children J.W and A.B., and all others harmed by Chord's misconduct.

8. The exposure of one's PII/PHI to cybercriminals is a bell that cannot be unrung. Before this data breach, its current and former patients' private information was exactly that—private. Not anymore. Now, their private information is forever exposed and unsecure.

[2] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited April 03, 2025).

PARTIES

9. Plaintiff, Andrea Rawlinson, is a natural person and citizen of Pennsylvania. She resides in Philadelphia, Pennsylvania where she intends to remain.

10. Defendnant CDHA Management, LLC is a Delaware corporation with its headquarters and principal place of business located in West Chester, PA.

11. Defendant Spark DSO, LLC is a Pennsylvania limited liability company with its headquarters and principal place of business located at 1801 West End Ave, Suite 410, Nashville, Tennessee 37203.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Defendant and Plaintiff are citizens of different states. And there are over 100 putative Class members.

13. This Court has personal jurisdiction over Defendant because it is a citizen in this District and maintains its headquarters and principal place of business in this District.

14. Venue is proper in this Court because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

BACKGROUND

Chord Collected and Stored the PII/PHI of Plaintiff and the Class

15. Defendant is a "Dental Support Organization dedicated to expanding access to quality dental care for children and adults, supporting over 60 practices across six states."[3]

[3] https://www.chordsdp.com/about/ (last visited April 03, 2025).

16. As part of its business, Chord receives and maintains the PII/PHI of thousands of its current and former patients.

17. In collecting and maintaining the PII/PHI, Chord agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class members themselves took reasonable steps to secure their PII/PHI.

18. Under state and federal law, businesses like Chord have duties to protect their current and former patients' PII/PHI and to notify them about breaches.

19. Chord recognizes these duties, declaring in its "Privacy Policy" that "[t]he privacy of your health information is important to us. We understand that your health information is personal, and we are committed to protecting it."[4]

20. It also acknowledges that it is required by law to:

a. "Maintain the privacy of your protected health information;" and

b. "Abide by the terms of our Notice that is currently in effect."[5]

21. It also states "We are required by law to notify you if the privacy or security of your health information has been breached. The notification will occur by first class mail within sixty (60) days of the event."[6]

22. Despite recognizing its duty to do so, on information and belief, Defendant has not implemented reasonably cybersecurity safeguards or policies to protect its patients' PII/PHI or supervised its IT or data security agents and employees to prevent, detect, and stop breaches of its

[4] https://www.chordsdp.com/privacy-policy/ (last visited April 03, 2025).
[5] *Id.*
[6] *Id.*

systems. As a result, Defendant leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to patients' PII/PHI.

Chord's Data Breach

23. On or about September 11, 2024, Defendant "discovered suspicious activity related to an employee's email account" resulting in the exposure of current and former patients' health records, which included information such as their "address, Social Security number, driver's license, bank account information, payment card information, date of birth, medical information, and health insurance information."[7]

24. Cybercriminals had access to Defendant's systems from August 19, 2024 until September 25, 2025—for more than an entire month.[8]

25. And yet, Chord waited until March 14, 2025, before it began notifying the class—almost an *eight months* after it discovered the Data Breach. Ex. A.

26. Thus, Chord kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

27. And when Defendant did notify Plaintiff and the Class of the Data Breach, it acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, encouraging Plaintiff and the Class to review the "Recommended Steps" document attached to the Breach Notice, and to "remain vigilant against incidents of identity theft and fraud." Ex. A.

28. Chord failed its duties when its inadequate security practices caused the Data Breach. In other words, Chord's negligence is evidenced by its failure to prevent the Data Breach

[7] https://www.chordsdp.com/notification-of-data-security-incident/ (last visited April 3, 2025).
[8] *Id.*

and stop cybercriminals from accessing the PII/PHI. And thus, Chord caused widespread injury and monetary damages.

29. Since the Data Breach, Chord has declared that it has "implemented additional technical safeguards." Ex. A. But this is too little too late. Simply put, these measures—which Chord now recognizes as necessary—should have been implemented *before* the Data Breach.

30. On information and belief, Chord failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures.

31. Chord has done little to remedy its Data Breach. Chord has offered victims credit monitoring and identity related services. However, such services are wholly insufficient to compensate Plaintiff and Class members for the injuries that Chord inflicted upon them.

32. Because of Chord's Data Breach, the PII/PHI of Plaintiff and Class members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiff and Class members.

33. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's Private Information. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

34. And as the Harvard Business Review notes, such "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[9]

[9] Brenda R. Sharton, *Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back.

35. Thus, on information and belief, Plaintiff's and the Class's stolen PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

Plaintiffs' Experiences and Injuries

36. Plaintiff Adrea Rawlinson's two minor children J.W. and A.B. are a current patients of Chord and a Data Breach victim.

37. Thus, on information and belief Chord obtained and maintained Plaintiff's minor children's PII/PHI.

38. As a result, Plaintiff's minor children were injured by Chord's Data Breach.

39. As a condition of receiving services with Defendant, Plaintiff provided Chord with her minor children's PII/PHI and allowed them to maintain that PII/PHI. Chord used their PII/PHI to facilitate its services.

40. Plaintiff trusted the company would use reasonable measures to protect her minor children's PII/PHI according to Chord's internal policies, as well as state and federal law. Chord obtained and continues to maintain Plaintiff's minor children's PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

41. Plaintiff reasonably understood that a portion of the funds she paid for services would be used to pay for adequate cybersecurity and protection of PII/PHI.

42. Plaintiff received a Notice of Data Breach from Defendant in or around March 2025.

43. Thus, on information and belief, Plaintiff's minor children's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

44. Through its Data Breach, Chord compromised Plaintiff's minor children's names, dates of birth, and medical information. Ex. A.

45. Plaintiff has spent—and will continue to spend—significant time and effort monitoring her and her minor children's accounts to protect them from identity theft and contacting counsel. After all, Chord directed Plaintiff to take those steps in its breach notice.

46. Plaintiff and minor children fear for the security of her minor children's PII/PHI and worries about what information was exposed in the Data Breach.

47. Because of Chord's Data Breach, Plaintiff and her minor children have suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's minor children's injuries are precisely the type of injuries that the law contemplates and addresses.

48. Plaintiff suffered actual injury from the exposure and theft of her minor children's PII/PHI—which violates her rights to privacy.

49. Plaintiff's minor children suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and medical identity theft—all because Chord's Data Breach placed Plaintiff's minor children's PII/PHI right in the hands of criminals.

50. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate her minor children's injuries.

51. Today, Plaintiff has a continuing interest in ensuring that her PII/PHI—which, upon information and belief, remains backed up in Chord's possession—is protected and safeguarded from additional breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

52. Because of Chord's failure to prevent the Data Breach, Plaintiff and Class members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary

losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their PII/PHI is used;

b. diminution in value of their PII/PHI;

c. compromise and continuing publication of their PII/PHI;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen PII/PHI; and

h. continued risk to their PII/PHI—which remains in Chord's possession—and is thus as risk for futures breaches so long as Chord fails to take appropriate measures to protect the PII/PHI.

53. Stolen PII/PHI is one of the most valuable commodities on the criminal information black market.

54. According to the National Association of Healthcare Access Management, "[p]ersonal medical data is said to be more than ten times as valuable as credit card information. PHI has such a high value because it contains highly sensitive information, such as social security numbers, birth dates, addresses, credit card numbers, telephone numbers and medical conditions.

This data is incredibly valuable on the black market because, unlike a stolen credit card that can be easily canceled, most people are unaware that their medical information has been stolen."[10]

55. According to Advent Health University, when an electronic health record "lands in the hands of nefarious persons the results can range from fraud to identity theft to extortion. In fact, these records provide such valuable information that hackers can sell a single stolen medical record for up to $1,000."[11]

56. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

57. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase Private Information on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

58. According to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals hack into medical practices for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents."[12]

---

[10] https://www.naham.org/page/ConnectionsThe-Value-of-Personal-Medical-Information#:~:text=Personal%20medical%20data%20is%20said,telephone%20numbers%20and%20medical%20conditions, (last visited April 03, 2025).
[11] https://www.ahu.edu/blog/data-security-in-healthcare (last visited April 03, 2025).
[12] https://www.hipaajournal.com/why-do-criminals-target-medical-records/ (last visited April 03, 2025).

59. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[13]

60. The HIPAA Journal article goes on to explain that patient records, like those stolen from Chord, are "often processed and packaged with other illegally obtained data to create full record sets (the previously mentioned Fullz package) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[14]

61. Data breaches such as the one experienced by Defendant have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, can prepare for, and hopefully can ward off a potential attack.

62. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[15]

63. These significant increases in attacks to companies, particularly those in the healthcare industry, and attendant risk of future attacks, is widely known to the public and to anyone in that industry, including Defendant Chord.

---

[13] *Id.*
[14] *Id.*
[15] https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited April 03, 2025).

64. A study by Experian found that the average total cost of medical identity theft is "nearly $13,500" per incident, and that many victims were forced to pay out-of-pocket costs for fraudulent medical care.[16] Victims of healthcare data breaches often find themselves "being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores."[17]

65. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

66. It is incorrect to assume that reimbursing a victim for a financial loss due to fraud makes that individual whole again. Similar to the GAO's study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, about a third (32%) spent a month or more resolving problems."[18] In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims."[19]

---

[16]https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last visited April 03, 2025).
[17]*Id.*
[18] https://bjs.ojp.gov/content/pub/pdf/vit14.pdf (last visited April 03, 2025).
[19] *Id.*

67. Further, once a patient's medical information is in the hands of thieves, they have access to the individual's health insurance and may use it to obtain free medical care, which can "ruin credit and take months, or even years, to resolve."[20]

68. As the fraudulent activity resulting from the Data Breach may not come to light for years, Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

Chord Knew—Or Should Have Known—of the Risk of a Data Breach

69. Chord's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

70. In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020.[21]

71. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[22]

---

[20] https://www.naham.org/page/ConnectionsThe-Value-of-Personal-Medical-Information#:~:text=Personal%20medical%20data%20is%20said,telephone%20numbers%20and%20medical%20conditions (last visited April 03, 2025).

[21] *See 2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) https://notified.idtheftcenter.org/s/.

[22] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

72. Chord's Data Breach follows a number of high-profile data breaches of US healthcare providers. This includes the Change Healthcare ransomware attack in February 2024, which has led to more than 100 million Americans' personal data being breached and a ransomware attack on Ascension in May in resulted in 5.6 million individuals having their sensitive personal, medical and financial information breached.[23]

73. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Chord's industry, including Defendant.

Chord Failed to Follow FTC Guidelines

74. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

75. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[24] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

[23] https://www.infosecurity-magazine.com/news/medusind-breach-patient-data/ (last visited April 03, 2025).

[24] *Protecting Personal Information: A Guide for Business,* FEDERAL TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

76. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

77. Furthermore, the FTC explains that companies must:

a. not maintain information longer than is needed to authorize a transaction;

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

f. verify that third-party service providers use reasonable security measures.

78. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

79. In short, Chord's failure to use reasonable and appropriate measures to protect against unauthorized access to its current and former patients' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Chord Failed to Follow Industry Standards

80. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-

malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

81. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

82. Upon information and belief, Chord failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04).

83. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Chord opened the door to the criminals—thereby causing the Data Breach.

Chord Violated HIPAA

84. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[25]

[25] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

85. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PHI and PHI is properly maintained.[26]

86. The Data Breach itself resulted from a combination of inadequacies showing Chord failed to comply with safeguards mandated by HIPAA. Chord's security failures include, but are not limited to:

a. failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. failing to ensure compliance with HIPAA security standards by Chord's workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to

[26] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

87. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Chord failed to comply with safeguards mandated by HIPAA regulations.

CLASS ACTION ALLEGATIONS

88. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing in the United States whose PII/PHI was compromised in the Data Breach including all those individuals who received notice of the breach.

89. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Chord has a controlling interest, any Chord officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

90. Plaintiff reserves the right to amend the class definition.

91. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

92. Ascertainability. All members of the proposed Class are readily ascertainable from information in Chord's custody and control. After all, Chord already identified some individuals and sent them data breach notices.

93. Numerosity. The Class members are so numerous that joinder of all Class members is impracticable. Upon information and belief, the proposed Class includes at least 173,430 members.

94. Typicality. Plaintiff's claims are typical of Class members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

95. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's common interests. Her interests do not conflict with Class members' interests. And Plaintiff has retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

96. Commonality and Predominance. Plaintiff's and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting

individual Class members—for which a class wide proceeding can answer for all Class members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Chord had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII/PHI;

b. if Chord failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. if Chord were negligent in maintaining, protecting, and securing PII/PHI;

d. if Chord breached contract promises to safeguard Plaintiff and the Class's PII/PHI;

e. if Chord took reasonable measures to determine the extent of the Data Breach after discovering it;

f. if Chord's Breach Notice was reasonable;

g. if the Data Breach caused Plaintiff and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiff and the Class are entitled to damages, treble damages, and or injunctive relief.

97. Superiority. A class action will provide substantial benefits and is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that individual litigation against Chord would require. Thus, it would be practically impossible for Class members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties

and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

98. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

99. Plaintiff and the Class entrusted their minor children's PII/PHI to Chord on the premise and with the understanding that Chord would safeguard their PII/PHI, use their PHI to provide services only, and not disclose their PII/PHI to unauthorized third parties.

100. Chord owed a duty of care to Plaintiff and Class members because it was foreseeable that Chord's failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII/PHI in a data breach. And here, that foreseeable danger came to pass.

101. Chord has full knowledge of the sensitivity of the PII/PHI and the types of harm that Plaintiff and the Class could and would suffer if their PII/PHI was wrongfully disclosed.

102. Chord owed these duties to Plaintiff and Class members because they are members of a well-defined, foreseeable, and probable class of individuals whom Chord knew or should have known would suffer injury-in-fact from Chord's inadequate security practices. After all, Chord actively sought and obtained Plaintiff's minor children's and Class members' PII/PHI.

103. Chord owed—to Plaintiff and Class members—at least the following duties to:

a. exercise reasonable care in handling and using the PII/PHI in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiff and Class members within a reasonable timeframe of any breach to the security of their PII/PHI.

104. Thus, Chord owed a duty to timely and accurately disclose to Plaintiff and Class members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiff and Class members to take appropriate measures to protect their PII/PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

105. Chord also had a duty to exercise appropriate clearinghouse practices to remove PII/PHI it was no longer required to retain under applicable regulations.

106. Chord knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII/PHI of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

107. Chord's duty to use reasonable security measures arose because of the special relationship that existed between Chord and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Chord with their confidential PII/PHI, a necessary part of obtaining services from Defendant.

108. The risk that unauthorized persons would attempt to gain access to the PII/PHI and misuse it was foreseeable. Given that Chord hold vast amounts of PII/PHI, it was inevitable that unauthorized individuals would attempt to access Chord's databases containing the PII/PHI — whether by malware or otherwise.

109. PII/PHI is highly valuable, and Chord knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII/PHI of Plaintiff and Class members' and the importance of exercising reasonable care in handling it.

110. Chord improperly and inadequately safeguarded the PII/PHI of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

111. Chord breached these duties as evidenced by the Data Breach.

112. Chord acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class members' PII/PHI by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the PII/PHI was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

113. Chord breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII/PHI of Plaintiff and Class members which actually and proximately caused the Data Breach and Plaintiff and Class members' injury.

114. Chord further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and Class members' injuries-in-fact.

115. Chord has admitted that the PII/PHI of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

116. As a direct and traceable result of Chord's negligence and/or negligent supervision, Plaintiff and Class members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

117. And, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

118. Chord's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII/PHI by criminals, improper disclosure of their PII/PHI, lost benefit of their bargain, lost value of their PII/PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Chord's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CLAIM FOR RELIEF
Negligence *per se*
(On Behalf of Plaintiff and the Class)

119. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

120. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

121. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as

Defendant, of failing to use reasonable measures to protect the PII entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the Class Members' sensitive PII.

122. Defendant breached its respective duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII.

123. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

124. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

125. Similarly, under HIPAA, Chord had a duty to follow HIPAA standards for privacy and security practices—as to protect Plaintiff's and Class members' PII/PHI.

126. Chord violated its duty under HIPAA by failing to use reasonable measures to protect its PII/PHI and by not complying with applicable regulations detailed *supra*. Here too, Chord's conduct was particularly unreasonable given the nature and amount of PII/PHI that Chord collected and stored and the foreseeable consequences of a data breach, including, specifically, the

immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

127. But for Defendant's wrongful and negligent breach of its duties owed, Plaintiff and Class Members would not have been injured.

128. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

129. Defendant's violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

130. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*)

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

131. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

132. Plaintiff and Class members were required to provide their PII/PHI or the PII/PHI of their minor children to Chord as a condition of receiving services provided by Defendant. Plaintiff and Class members provided their PII/PHI to Chord in exchange for Chord's services.

133. Plaintiff and Class members reasonably understood that a portion of the funds they paid Chord would be used to pay for adequate cybersecurity measures.

134. Plaintiff and Class members reasonably understood that Chord would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Chord's duties under state and federal law and its internal policies.

135. Plaintiff and the Class members accepted Chord's offers by disclosing PII/PHI to Chord in exchange for services.

136. In turn, and through internal policies, Chord agreed to protect and not disclose the PII/PHI to unauthorized persons.

137. In its Privacy Policy, Chord represented that they had a legal duty to protect Plaintiff's minor children's and Class Member's PII/PHI.

138. Implicit in the parties' agreement was that Chord would provide Plaintiff and Class members with prompt and adequate notice of all unauthorized access and/or theft of PII/PHI.

139. After all, Plaintiff and Class members would not have entrusted PII/PHI to Chord in the absence of such an agreement with Defendant.

140. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

141. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

142. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

143. Chord materially breached the contracts it entered with Plaintiff and Class members by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII/PHI that Chord created, received, maintained, and transmitted.

144. In these and other ways, Chord violated its duty of good faith and fair dealing.

145. Chord's material breaches were the direct and proximate cause of Plaintiff's and Class members' injuries (as detailed *supra*).

146. And, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

147. Plaintiff and Class members performed as required under the relevant agreements, or such performance was waived by Chord's conduct.

FOURTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

148. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

149. This claim is pleaded in the alternative to the breach of implied contract claim.

150. Plaintiff and Class members conferred a benefit upon Defendant. After all, Chord benefitted from using their PII/PHI to provide services and benefitted from the payment provided in exchange for services.

151. Chord appreciated or had knowledge of the benefits it received from Plaintiff and Class members.

152. Plaintiff and Class members reasonably understood that Chord would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Chord's duties under state and federal law and its internal policies.

153. Chord enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class members' PII/PHI.

154. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Chord instead calculated to avoid its data security obligations at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Chord's failure to provide the requisite security.

155. Under principles of equity and good conscience, Chord should not be permitted to retain the full value of Plaintiff's and Class members' payment because Chord failed to adequately protect their PII/PHI.

156. Plaintiff and Class members have no adequate remedy at law.

157. Chord should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class members—all unlawful or inequitable proceeds that it received because of its misconduct.

FIFTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

158. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

159. Given the relationship between Chord and Plaintiff and Class members, where Chord became guardian of Plaintiff's and Class members' PII/PHI, Chord became a fiduciary by its undertaking and guardianship of the PII/PHI, to act primarily for Plaintiff and Class members, (1) for the safeguarding of Plaintiff and Class members' PII/PHI; (2) to timely notify Plaintiff and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Chord did and does store.

160. Chord has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of Chord's relationship with them—especially to secure their PII/PHI.

161. Because of the highly sensitive nature of the PII/PHI, Plaintiff and Class members would not have entrusted Defendant, or anyone in Chord's position, to retain their PII/PHI had they known the reality of Chord's inadequate data security practices.

162. Chord breached its fiduciary duties to Plaintiff and Class members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class members' PII/PHI.

163. Chord also breached its fiduciary duties to Plaintiff and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

164. As a direct and proximate result of Chord's breach of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

PRAYER FOR RELIEF

Plaintiff and Class members respectfully request judgment against Chord and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;

B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Chord from further unfair and/or deceptive practices;

E. Awarding Plaintiff and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all claims so triable.

Date: April 3, 2025

Respectfully submitted,

By: /s/ *J. Gerard Stranch, IV*
J. Gerard Stranch, IV, BPR 23045
Grayson Wells, BPR 39658
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Ave., Ste. 200
Nashville, TN 37203
Tel: (615) 254-8801
gstranch@stranchlaw.com
gwells@stranchlaw.com

Raina Borrelli*
STRAUSS BORRELLI, PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
T: (872) 263-1100
F: (872) 263-1109
raina@straussborrelli.com

**Pro hac vice forthcoming*

Counsel for Plaintiff and Proposed Class